

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**



AIR FORCE INSTRUCTION 14-128

28 SEPTEMBER 2010

**AIR FORCE ISR AGENCY
Supplement**

2 AUGUST 2011

Intelligence

**AIR FORCE SERVICE CRYPTOLOGIC
COMPONENT (AF SCC)**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR:

Certified by: AF/A2RN
(Mr. Kenneth Dumm)

Pages: 18

(AFISRA)

OPR: AFISRA/A3O

Certified by: AFISRA/A3 (Col Joseph T.
Dinuovo)

Supersedes: AFISRAI 10-102, 14
November 2007

Pages: 7

The purpose of this instruction is to define the roles, responsibilities, relationships, and functions of the Air Force Service Cryptologic Component (AF SCC) and implement Executive Order, DoD, USAF, Intelligence Community (IC) and NSA/CSS directives and guidance.

This instruction provides guidance on the roles, responsibilities, relationships, and functions of the Air Force Service Cryptologic Component (AF SCC). It implements Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources and Operations*; Headquarters Air Force Mission Directive (HAFMD) 1-33,

Deputy Chief of Staff of the Air Force, Intelligence, Surveillance, and Reconnaissance; Department of Defense Instruction (DoDI) O-3115.07, *Signals Intelligence (SIGINT)*; Department of Defense Directive DoDD5100.20, *DoD Intelligence Activities, National Security Agency/Central Security Service (NSA/CSS)*; NSA/CSS Policy 1-3; Air Force Doctrine Document (AFDD) 2-9, *Intelligence, Surveillance, and Reconnaissance (ISR) Operations*; Air Force Mission Directive (AFMD) 15, *Air Force Intelligence, Surveillance, and Reconnaissance*

Agency (AF ISR Agency); Air Force Instruction 38-204, *Programming USAF Manpower*; Headquarters United States Air Force (HQ USAF) Program Action Directive (PAD) 07-08 Change 4, and other higher headquarters (HHQ) directives and National Intelligence Community guidance. This AFI applies to all active USAF Organizations, Air Force Reserve Command (AFRC) and Air National Guard (ANG) units. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through the appropriate functional's chain of command. Field activities must send implementing publications to the higher headquarters functional OPR for review and coordination before publishing. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Disposition Schedule (RDS) located at <https://www.mv.af.mil/afirms/afirms/afirms/rims/cfm>. This publication may require the collection and or maintenance of information protected by the Privacy Act (PA) of 1974. The authorities to collect and or maintain records prescribed in this publication are Title 37 *United States Code*, Sections 8013 and 9832, Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons, November 22, 1943 as amended by Executive Order 13478, Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers, November 18, 2008, and AFD 14-1, *Intelligence, Surveillance, and Reconnaissance Planning, Resources*, and AFD 14-3, *Control, Protection and Dissemination of Intelligence Information*."

OVERVIEW

In 1948, the United States Air Force Security Service (USAFSS) was created as a single-service organization for USAF cryptologic capabilities. Along with sister service counterparts, this single organization was referred to as a Service Cryptologic Element (SCE) in National Security Agency and Department of Defense guidance and policy, and assigned numerous roles and responsibilities in support of a unified US cryptologic enterprise. Through the years, successor AF organizations also assumed the SCE role: Electronic Security Command, AF Intelligence Command, and Air Intelligence Agency. In 2001, changes in AF organization created the situation where some AF cryptologic capabilities, manpower and resources were no longer assigned directly to the AF SCE. In 2007, Director NSA policy changed SCE to Service Cryptologic Component (SCC); simultaneously the Air Force transformed Air Intelligence Agency to AF Intelligence, Surveillance and Reconnaissance Agency (AF ISR Agency) through PAD 07-09. PAD 07-09 and later AF Mission Directive 15, *Air Force Intelligence, Surveillance, and Reconnaissance Agency (AF ISR Agency)* re-designated AF ISR Agency as the AF SCC. All of these changes, along with the existence of some cryptologic capabilities not assigned to the AF SCC, highlighted the urgent requirement for an AF Instruction to specify the roles and responsibilities of the AF SCC and AF organizations that would support Department of Defense requirements for the Service Cryptologic Component.

| | | |
|----|--------------------------------|---|
| 1. | AF SCC Role. | 3 |
| 2. | AF SCC Responsibilities: | 3 |

| | | |
|----|---|----|
| 3. | Air Force Cryptologic Office (AFCO) Responsibilities: | 8 |
| 4. | USAF Organization Responsibilities: | 10 |

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 14

1. AF SCC Role. AF SCC is the principal advisor to the AF/A2 staff for all programming, budgeting, training, personnel, policy, doctrine, governance, and foreign relationships for USAF cryptologic activities. The AF SCC ensures compliance by all USAF cryptologic activities with the cryptologic policies, tasking, and technical guidance provided by DoD and the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS).

2. AF SCC Responsibilities: The AF SCC is the service lead for all USAF cryptologic activities and has management oversight of those elements of the USAF performing cryptologic functions. This applies to the cryptologic staff of the AF ISR Agency, its subordinate elements, and cryptologic elements assigned to other USAF organizations. The AF ISR Agency Commander is the AF SCC/CC and principal USAF advisor to DIRNSA/CHCSS for USAF cryptologic matters. The AF SCC maintains an appropriate staff to organize train and equip all cryptologic resources and activities in the USAF. This staff also provides the management oversight for all USAF cryptologic activities regardless of program to ensure these activities are compliant with National and Departmental guidelines, including SIGINT security, training, authorities, accountability of resources, and oversight (inspections, skill evaluations, and reporting).

2.1. Guidance and policy for the management of cryptologic activities come from various sources at different levels. AF SCC remains current on all these guidance and policy documents to ensure USAF cryptologic activities are conducted within the parameters established by them.

2.1. (**AFISRA**) The Commander, HQ AFISRA (AFISRA/CC) delegates operational oversight and functional management to the HQ AFISRA Director of Intelligence (A2) and Director of Operations (A3). As the AF SCC Director of Intelligence and Director of Operations, AFISRA/A2 and AFISRA/A3 exercise SCC oversight responsibility for USAF cryptologic operational activities. SCC oversight is comprised of two primary functions: implementing the legal authority to conduct SCC cryptologic missions on behalf of the NSA/CSS and monitoring the execution of cryptologic missions. Functional management includes all organize, train, and equip functions of all USAF cryptologic activities regardless of program to ensure these activities are postured to accomplish the mission and compliant with existing guidance and policy. **Note:** AFISRA will coordinate and deconflict with the command exercising primary ADCON when executing SCC management oversight over cryptologic elements assigned outside of AFISRA.

2.1.1. Execute AF/A2 responsibilities ensuring proper supervision and administrative/technical control of USAF cryptologic intelligence activities, to include leading implementation of cryptologic tasking, planning, collection, processing and exploitation, analysis dissemination and interoperability between existing and future USAF, other Military Department, NSA/CSS, and USSOCOM SIGINT systems; seamless connectivity between national and tactical systems; and modernization of cryptologic systems.

2.1.1. **(AFISRA)** AFISRA/CC will maintain overall responsibility for all Air Force participation in cryptologic operations. AFISRA/A2 will provide oversight and guidance for SIGINT Intelligence Oversight, National-Tactical Integration (with coordination from AFISRA/A5/8/9), Tactics Analysis and Reporting Program, Global Aviation Analysis Support Team, and all second and third phase cryptologic analysis activities. AFISRA/A3 will provide oversight and guidance for intelligence planning and direction, collection, processing and exploitation, analysis, production and dissemination, mission management, cryptologic training and position certification, cryptologic support to military operations and electronic combat, and other activities as appropriate. AFISRA/A4/7 will provide oversight and guidance for logistical and maintenance issues, and other activities as applicable. AFISRA/A5/8/9 will provide oversight and guidance for planning, acquisition, and requirements issues, and other activities as applicable. AFISRA/A6 will provide oversight and guidance for communications infrastructure and computer issues, and other activities as applicable. AFISRA/ZQ will provide oversight and guidance for collection/analysis/reporting related to specialized ISR support to cryptologic Air Force Space Control and Network Warfare Special Access Programs, and other activities as applicable.

2.1.1.1. Ensure USAF elements engaged in cryptologic activities comply with the Constitution, Federal law, Executive Orders, DoD, and DIRNSA/CHCSS policies and guidance.

2.1.2. Command and manage subordinate cryptologic units. Provide guidance, assistance, and management oversight to USAF and ARC elements assigned to other commands when engaged in cryptologic activities, to ensure proper application of resources, synchronization of cryptologic missions, and compliance with applicable guidance.

2.1.3. Lead USAF efforts to resolve cryptologic intelligence deficiencies working with the Headquarters Air Force (HAF), National IC organizations, Service laboratories, training organizations, and operating and implementing commands.

2.1.4. Coordinate with AF/A2 and USAF organizations to satisfy personnel requirements identified by DIRNSA/CHCSS.

2.1.5. Articulate DIRNSA/CHCSS mission/capability requirements to AF/A2 and USAF organizations engaged in cryptologic activities.

2.1.6. Provide the IC and USAF/Joint customers with cryptologic intelligence products, applications, services, and cryptologic intelligence expertise in the areas of Signals Intelligence (SIGINT), Information Assurance (IA), acquisition, foreign weapons systems and technology, and treaty monitoring.

2.1.7. **(Added-AFISRA)** Coordinate Tactical/National SIGINT requirements and issues at all levels: national agencies, service, and intermediate-level headquarters.

2.1.8. **(Added-AFISRA)** Publish Compliance and Standardization Requirements List (C&SRL) (or applicable inspection criteria) to facilitate effective inspections of cryptologic mission areas to include, but not limited to: Mission Management, Analysis and Reporting, Threat Warning, National Tactical Integration and Cryptologic Operations.

2.1.9. **(Added-AFISRA)** Provide ISR operations support to Air Force research, development, test, sustainment and planning activities IAW AFI 14-111, *Intelligence in Force Modernization*.

2.1.10. **(Added-AFISRA)** Coordinate the development and validation of AFISRA SIGINT Unit Type Codes (UTCs) and Designated Operational Capability Statements.

2.1.11. **(Added-AFISRA)** Serve as an AF ISR cryptologic operations focal point for deliberate planning and the review and evaluation of the Intelligence annexes within Joint Chiefs of Staff (JCS) and Higher Headquarters (HHQ) wartime Operational Plans (OPLANs), policy and guidance. IAW AFI 14-202 Volume 3, *General Intelligence Rules*.

2.2. Security, while important across the entire spectrum of intelligence activities, has increased emphasis and requirements within the cryptologic realm. To ensure USAF cryptologic activities adhere to the guidance and policies surrounding cryptologic missions, AF SCC will:

2.2.1. Ensure the USAF cryptologic workforce is trained to DIRNSA/CHCSS-established standards and appropriately cleared to perform duties across the USAF cryptologic enterprise.

2.2.2. Execute the AF SCC certification and accreditation process as Designated Approval Authority representative on behalf of DIRNSA/CHCSS for sensitive compartmented information systems and cryptologic intelligence systems.

2.2.2.1. Engineer, install, operate, and maintain NSA specialized communication equipment, systems, and infrastructure.

2.2.2.2. Process validated requests for access to NSA special communications systems.

2.2.2.3. Plan, schedule and conduct JTIDS tactical data link certification testing for Special Information Systems.

2.2.2.4. **(Added-AFISRA)** Publish mission-specific security classification guidance as required and when appropriate. AFISRA/SO will act as OPR for this function.

2.3. Cryptologic skills and equipment are unique and critical to the success of military operations throughout the world. Specific standards are established for the various cryptologic mission functions. To ensure that the USAF cryptologic workforce meets these standards, the AF SCC will:

2.3.1. Sustain USAF cryptologic readiness by developing and maintaining a cryptologic force structure with the proper rank and specialty allocations of military and civilian personnel, training and educating mission-ready cryptologic professionals, regularly exercising cryptologic wartime system capabilities, and equipping and maintaining an infrastructure capable of supporting high operations tempo levels.

2.3.1. **(AFISRA)** Oversee AFISRA's operational readiness, customer requirements and support, and measurements necessary to assess the effectiveness of support provided.

2.3.1.1. For personnel assigned to AF ISR Agency, organize, train, equip, present, and integrate USAF cryptologic and full-spectrum ISR capabilities to the IC, and to

the USAF/Joint/Coalition commanders in support of combatant commands. For personnel not assigned to the AF ISR Agency, train, equip, and certify personnel and units via inspections and evaluations to conduct cryptologic operations in accordance with DIRNSA/CHCSS guidance.

2.3.1.2. Disseminate DIRNSA/CHCSS guidance to all USAF elements engaging in cryptologic activities on military and civilian career development and training programs, developing cryptologic knowledge and skill standards, and the availability of DIRNSA/CHCSS –sponsored specialized and advanced cryptologic training opportunities.

2.3.1.3. Provide guidance on training standards for all USAF cryptologic intelligence personnel and for unit external cryptologic intelligence training.

2.3.1.4. Annually solicit cryptologic units' formal training requirements for the subsequent year and coordinate with appropriate agencies.

2.3.1.5. Annually provide an AF SCC-sponsored list of recommended cryptologic training opportunities to increase USAF cryptologic elements awareness of available training courses.

2.3.1.6. **(Added-AFISRA)** Provide assistance to subordinate AFISRA operational units, and other non-AFISRA USAF units performing cryptologic missions, in addressing operational-related training, manpower, equipment, communication requirements, and issues.

2.3.2. Provide direct support to the cryptologic force modernization process working as lead agency to identify and resolve system and infrastructure deficiencies.

2.3.2.1. Provide a common understanding of cryptologic program/initiative intelligence needs across the intelligence, acquisition, and other operations communities. Create a working familiarity of the cryptologic intelligence infrastructure and threat analysis among acquisition/operational authorities and their associated intelligence stakeholders.

2.3.2.2. Ensure stakeholders involved with intelligence support to acquisition are integrated into planning, programming, and decision activities to weigh costs/benefits/tradeoffs.

2.3.2.3. Provide an ability to analyze and compare a variety of intelligence requirements and deficiencies across numerous programs/initiatives to support the recommendation and advocating of prioritized, efficient solutions at reasonable cost.

2.3.3. Provide technical advice, guidance, and obtain DIRNSA/CHCSS assistance, consistent with enterprise architecture and interoperability standards established by the IC CIO, to USAF organizations engaged in SIGINT RDT&E investment programs. This ensures the architecture, standards, and interoperability between existing and future USAF, other Military Departments, and USSOCOM SIGINT; connectivity between national and tactical systems; and modernization of systems provide seamless interoperability now and in the future.

- 2.3.3.1. Provide guidance on cryptologic architectures, cryptologic intelligence products (e.g. data bases and tools), and other cryptologic intelligence matters to USAF requirements and acquisition customers, as applicable.
- 2.3.3.2. Guide the USAF development of network-enabled SIGINT equipment that meets architecture standards and is interoperable with national SIGINT systems, other Military Department tactical SIGINT systems, and JIOC operating systems, as necessary.
- 2.4. To conduct cryptologic activities, certain authorities must be in place prior to performing those missions. These authorities are non-transferable across USAF units and are normally determined by DIRNSA/CHCSS. To ensure USAF cryptologic activities operate under correct authorities, the AF SCC will:
 - 2.4.1. Ensure USAF elements do not engage in SIGINT activities without approved direction or delegation by the SECDEF or DIRNSA/CHCSS, or as otherwise provided for in NSCID 6.
 - 2.4.2. Ensure compliance with DIRNSA/CHCSS SIGINT instructions on planning, collection, processing and exploitation, analysis, and dissemination. These instructions are mandatory for all DoD Components conducting SIGINT under Secretary of Defense (SECDEF) authority unless directed otherwise by SECDEF.
- 2.5. The AF SCC fully engages with HAF on the planning, programming, budgeting, and execution of the Consolidated Cryptologic Program (CCP). AF SCC must also synchronize the cryptologic programs throughout the USAF for efficiency and effectiveness in meeting USAF requirements. To ensure the proper programming and distribution of USAF cryptologic resources, the AF SCC will:
 - 2.5.1. Articulate AF/A2 approved cryptologic-related requirements, issues, and interests to DIRNSA/CHCSS, Mission Resource Authorities (MRAs), and Senior Functional Authorities (SFAs).
 - 2.5.2. Act as site advocate, where designated, coordinating with SFAs and local military authorities for the negotiation and execution of support agreements.
 - 2.5.3. Provide the AF/A2 - approved input to, and participate fully in, NSA/CSS corporate processes on planning, programming, and budgeting of manpower and other resources for mission, mission support, and, as required, base operations support.
- 2.6. Management oversight is the authority to determine if applicable guidance and policy are implemented as intended. SCC management oversight is irrespective of command assignment of billets. To ensure compliance with guidance and policy, the AF SCC will:
 - 2.6.1. Coordinate and conduct joint intelligence staff assistance visits and inspections to ensure USAF organizations comply with this instruction and with applicable policies and guidance.
 - 2.6.2. Conduct regular inspections of cryptologic activities for compliance with the law, executive orders, and related directives.
 - 2.6.2.1. Ensure Intelligence Oversight (IO), and security reporting procedures are followed by USAF cryptologic elements regarding their activities and practices and

that periodic intelligence oversight reports and reports of questionable/sensitive activities are submitted as appropriate in NSA and Air Force channels.

2.6.2.2. On Intelligence Oversight matters, consult with NSA General Counsel and IG and AF General Counsel and IG on matters involving interpretations or possible violations of law, executive orders or directives.

2.6.2.3. Provide legal advice and assistance to all USAF cryptologic elements.

2.6.2.4. **(Added-AFISRA)** Ensure all units document annual compliance and Quarterly and Event Reporting with Intelligence Oversight training in accordance with NSA/CSS Policy 1-23, *Procedures Governing NSA/CSS Activities that Affect U.S. Persons* and, USSID SP0018, *Legal Compliance and Minimization Procedures* for SIGINT field activities.

2.6.3. Conduct a periodic review of USAF cryptologic activities and practices to ensure consistency with laws, authorities, policies, and guidance on cryptologic-unique issues.

2.6.4. **(Added-AFISRA)** Ensure all units are thoroughly familiar with Critical Information (CRITIC) handling responsibilities and ensure units conduct regular CRITIC Training and Evaluation (CTEP) IAW USSID CR1501, *Handling of Critical Information (CRITIC)* and AFISRAI 14-105, *CRITIC Program Management*.

2.6.5. **(Added-AFISRA)** Provide guidance, assistance, and management oversight to USAF and ARC elements integral to other commands when engaged in cryptologic activities, to ensure proper application of resources, synchronization of cryptologic missions, and compliance with applicable cryptologic mission guidance.

2.6.5.1. **(Added-AFISRA)** Review, at least quarterly, Intercept Tasking Data Base (ITDB) messages affecting Air Force airborne ISR sensors and provide any suggested ITDB modifications to the NSA Airborne Collection Management Branch for consideration. AFISRA/A3O is OPR.

2.6.5.2. **(Added-AFISRA)** Review all Combatant Command (COCOM) and Combatant-Numbered Air Force (C-NAF) formal tasking messages, such as Collection Emphasis Messages (CEM), SIGINT Emphasis Tasking Messages (SETM), and Reconnaissance and Surveillance Targeting Annex (RSTA), affecting Air Force airborne ISR sensors and provide any suggested CEM/SETM/RSTA modifications to the appropriate COCOM/C-NAF.

2.6.6. **(Added-AFISRA)** Convene conferences and technical exchanges as needed to coordinate and synchronize cryptologic mission activities.

2.6.7. **(Added-AFISRA)** Lead efforts as OPR on AFISRA instructions governing support, management, and execution of all ISR operations specific to their designed operating capability (e.g., Distributed Common Ground Systems, RC-135, etc.). AFISRA/A3O will act as OPR for ISR operational guidance.

3. Air Force Cryptologic Office (AFCO) Responsibilities: AFCO, located within Headquarters, NSA/CSS, Fort George G. Meade, MD, is designated as the AF SCC's principal representative to NSA/CSS and also functions as adjunct cryptologic staff to AF/A2. AFCO develops, leverages, and integrates USAF cryptologic capabilities and resources (national and tactical) to satisfy Joint, Total Force, and combatant commander requirements. AFCO will:

3.1. Provide management oversight of USAF organizations conducting cryptologic air, space or cyber intelligence missions, in coordination with other MAJCOMs, as appropriate, to ensure the USAF is postured to meet National and combatant commander cryptologic operations requirements IAW policy and guidance.

3.1.1. Coordinate USAF cryptologic policies, plans, and programs within the United States Cryptologic System (USCS) and the United States SIGINT System (USSS).

3.1.2. Ensure all USAF cryptologic mission documentation complies with NSA/CSS policy and governance.

3.1.3. Create, in coordination with AF SCC and USAF organizations, cryptologic governance and policy documentation, CONOPs, and MOUs/MOAs for all USAF cryptologic mission areas and guide them through the NSA/CSS process for approval.

3.2. Manage Cryptologic Oversight and Compliance responsibilities on behalf of AF SCC for all USAF cryptologic activities. Provide guidance and direction for all USAF incident and periodic quarterly reports for the NSA/IG and AF/GC and IG.

3.3. Be the USAF focal point for Exercise SIGINT and cryptologic system technology demonstration waivers.

3.3.1. Guide the development of USAF cryptologic plans, programs, missions, and technology integration.

3.3.1.1. Assist USAF elements in implementing cryptologic plans, policy, doctrine, and programs.

3.3.2. Lead SIGINT technology integration for all USAF activities receiving new technologies to perform SIGINT activities.

3.3.2.1. As designated by DIRNSA/CHCSS, coordinate for all field deployments of NSA/CSS-developed systems.

3.3.2.2. As designated by DIRNSA/CHCSS, perform provisional test director duties for NSA/CSS-deployed systems to USAF activities and lead site acceptance test and evaluation efforts.

3.4. Represent the USAF, both within NSA/CSS, and to the larger National Intelligence Community for cryptologic issues.

3.4.1. Advise AF SCC and AF/A2 in validating and prioritizing USAF cryptologic requirements and advocate these positions within NSA/CSS and to the IC.

3.4.2. Be the principal USAF entry point into NSA/CSS.

3.4.3. Advocate for established USAF cryptologic mission activities and coordinate USAF cryptologic mission development and integration with national SIGINT systems (e.g., AF-NTI, AF DCGS, Expeditionary SIGINT).

3.4.4. Oversee the USAF SIGINT RDT&E program.

3.4.4.1. Coordinate USAF SIGINT RDT&E requirements with DIRNSA/CHCSS.

3.4.4.2. Coordinate with appropriate Air Force organizations to ensure specified USAF SIGINT RDT&E tasks are accomplished within approved programs as requested by DIRNSA/CHCSS and IAW DoD guidance and direction.

3.4.4.3. Coordinate with appropriate Air Force organizations to ensure USAF SIGINT RDT&E and acquisition programs incorporate SIGINT threat countermeasures by performing threat analysis and coordination with other DoD Components, as necessary.

3.4.4.4. Coordinate with DIRNSA/CHCSS for SIGINT-expertise for research, development, testing and evaluation of USAF developed systems.

3.4.5. As designated by DIRNSA/CHCSS, perform duties as the Designated USSID Representative (DUR) for the USAF.

3.4.6. Per NSA/CSS direction, sponsor USAF requests for access to NSA sensitive databases.

3.5. Present the AF/A2 - approved submission of the USAF Consolidated Cryptologic Program (CCP) to DIRNSA/CHCSS.

3.5.1. Develop and manage the USAF portion of the NSA-developed Human Resources Management System (HRMS).

3.6. Support SAVs and inspections as required.

4. USAF Organization Responsibilities: USAF organizations engaged in cryptologic activities (MAJCOM, NAF, AFRC, ANG, and USAF educational and laboratories conducting cryptologic research) coordinate new cryptologic operation activities with AF SCC prior to starting initial implementation or prior to a change in mission. USAF Organizations will:

4.1. Coordinate cryptologic plans, policy, doctrine, governance, and foreign relationships with the AF SCC to ensure they are IAW applicable authorities, policy and guidance.

4.1.1. Coordinate with the AF SCC prior to engaging in SIGINT activities.

4.1.2. Coordinate with AFCO to ensure all cryptologic mission documentation complies with NSA/CSS policy and governance.

4.2. Provide required incident and periodic Intelligence Oversight reports pertaining to cryptologic matters to AF SCC. AF SCC will communicate with SAF IG/GC.

4.3. Ensure intelligence oversight training is accomplished as required by NSA and USAF.

4.4. Train their cryptologic workforce to DIRNSA/CHCSS-established standards to perform duties across the USAF cryptologic enterprise.

4.4.1. Provide cryptologic units' formal training requirements for the subsequent year to the AF SCC.

4.5. Coordinate with AFCO on all SIGINT-related research and development activities.

4.5.1. Coordinate with AFCO for access to NSA systems.

4.5.2. Receive delegation by the SECDEF or DIRNSA/CHCSS or as otherwise provided for in NSCID 6.

- 4.6. Provide requested resource data IAW AF/A2 provided guidance.
- 4.7. Coordinate and conduct joint intelligence staff assistance visits and inspections with AF SCC IG.
- 4.8. Provide to HAF/A2 for validation and submission to DIRNSA/CHCSS cryptologic resource requirements, including CCP requirements.
- 4.9. **(Added-AFISRA)** Provide ISR operations support to force protection in accordance with (IAW) AFI 14-119, *Intelligence Support to Force Protection*.

4.10. (AFISRA) AFISRA organizations and USAF, ANG, and AFRC organizations performing /participating in cryptologic operations (Added) These organizations are responsible for executing ISR activities in compliance with this instruction, statutes, and cryptologic directives, while overseeing the day-to-day operations and qualification and training of subordinate units and extended enterprise units. Extended enterprise units include temporarily established units subordinate to combatant commands and primarily sourced by personnel resources from existing cryptologic units; operational-level force provider units retain SIGINT technical control responsibility for the cryptologic activities of extended enterprise units. These units will:

- 4.10.1. **(Added-AFISRA)** Publish unit-specific supplementary guidance as necessary. Provide one informational copy of all instructions to HQ AFISRA/A2/A3 no later than 30 days from date of publication.
- 4.10.2. **(Added-AFISRA)** Ensure USSID site profiles are updated and relevant to current mission activities IAW USSID SP0002, *The USSID System*.
- 4.10.3. **(Added-AFISRA)** Maintain current awareness of field unit operations by performing or monitoring staff assistance visits, maintaining a working knowledge of unit operating instructions, and promoting effective exchanges between group and unit POCs.
- 4.10.4. **(Added-AFISRA)** Apprise HQ AFISRA of all issues requiring AF SCC attention:
 - 4.10.4.1. **(Added-AFISRA)** Units performing SIGINT or cryptologic missions will compile and submit not later the 5th duty day of the following month, to HQ AFISRA, a monthly narrative operational activity report tailored to the mission set. Activity reports will include critical training shortfalls, significant mission highlights, experienced or expected ops tempo issues, and production metrics (e.g., number of missions conducted/supported, number of reports issued, system outages, etc.), as applicable. Units may add information not listed above, but all information should provide insight to functional managers on the overall capability of ISR units to perform their assigned mission. Functional managers will provide specific guidance on format and vehicle.
 - 4.10.4.2. **(Added-AFISRA)** Identify and report ISR training program shortfalls that adversely impact cryptologic capabilities as soon as feasible.
- 4.10.5. **(Added-AFISRA)** Publish and coordinate Crew Manning Letters (CML) delineating the ISR crew complement (type and number of personnel) determined by the operational authority required to accomplish the ISR tasking at hand. CMLs will be validated by AFISRA/A3 but waiver authority to perform operations with a reduced crew

complement will be delegated to the appropriate operations group. AFISRA/A3O will be notified of reduced crew complement and projected impact upon tasking. Refer to AFISRAI 14-227, when published, for applicability and specific guidance on CMLs. **Note:** Air Force Space Command and 361 ISRG are exempt from CML requirement.

4.10.5.1. **(Added-AFISRA)** Ensure CMLs are sufficient to meet applicable operational tasking for each track/area supported and forward all CMLs to AFISRA/A3O for validation.

4.10.5.2. **(Added-AFISRA)** Build minimum crew manning on CMLs to ensure unit meets operational tasking for each area/track within their AOR in accordance with tasking found in Intercept Tasking Data Base (ITDB), Reconnaissance Surveillance Target Acquisition (RSTA) annexes, Collection Emphasis Messages (CEM), and guidance from applicable Target Offices of Primary Interest (TOPIs).

4.10.6. **(Added-AFISRA)** Ensure the development of subordinate field unit ISR training programs based on higher headquarters and national requirements ensuring members maintain proficiency.

4.10.6.1. **(Added-AFISRA)** Ensure subordinate field units maintain individual training and certification records on all cryptologic positions and perform an annual review.

4.10.6.2. **(Added-AFISRA)** Ensure qualification/certification of cryptologic personnel is IAW established NSA/CSS, AF, AFISRA, NAF and organizational instructions and applicable USSIDs.

4.10.7. **(Added-AFISRA)** Coordinate cryptologic operational issues, policies, requirements, and taskings with appropriate subordinate elements on a recurrent basis. Elevate problems/issues that cannot be resolved to HQ AFISRA as soon as feasible.

4.10.8. **(Added-AFISRA)** Perform annual self-assessments using a locally created self-inspection checklist IAW this instruction. Self-inspection checklists will be included in any unit supplements to this instruction. Provide one informational copy of all instructions to AFISRA/A2/A3 no later than 30 days from date of publication.

4.10.8.1. **(Added-AFISRA)** As necessary, request staff assistance visits from HQ AFISRA via official memorandum.

4.10.9. **(Added-AFISRA)** Review AFISRA/IG reports from various Wing, Center, Group, Squadron, and other Operational Readiness/Unit Compliance Inspections. Identify areas of cross-tell value and conduct lateral information sharing as required.

JAMES O. POSS, Maj Gen, USAF
Acting Deputy Chief of Staff, Intelligence,
Surveillance and Reconnaissance

(AFISRA)

BRADLEY A. HEITHOLD, Maj Gen, USAF
Commander

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

(Added-AFISRA) AFMAN 33-363, Management of Records, 18 May 2006

(Added-AFISRA) AFISRAI 14-105, CRITIC Program Management, 30 March 2006

(Added-AFISRA) AFI 14-111, *Intelligence in Force Modernization*, 23 January 2009

(Added-AFISRA) AFI 14-119, *Intelligence Support to Force Protection*, 15 August 2007

(Added-AFISRA) AFI 14-202, Volume 3, *General Intelligence Rules*, 10 March 2008

(Added-AFISRA) AFI 33-360, *Publications and Forms Management*, 18 May 06

(Added-AFISRA) AFI 33-360/AFISRA Supplement, 13 January 2010

AFPD 14-1, *Intelligence, Surveillance, and Reconnaissance Planning, Resources, and Operations*, 2 April 2004

AFPD 14-3, *Control, Protection and Dissemination of Intelligence Information*, 1 May 1998

AFI 14-104, *Oversight of Intelligence Activities*, 16 April 2007

AFI 14-105, *Unit Intelligence Mission and Responsibilities*, 3 June 2002

AFI 36-2201, *Air Force Training Program*, 4 February 2005

AFI 14-108, *AF Management of General Defense Intelligence Program (GDIP) Resources*, 25 Sep 2003

AFI 14-125, *Cryptologic Skills Program*, 30 July 2008

AFI 14-201, *Intelligence Production and Applications*, 1 Dec 2002

AFI 14-202v3, *General Intelligence Rules*, 10 Mar 2008

AFI 38-204, *Programming USAF Manpower*, 1 Aug 1999

DoDD 5100.20, *National Security Agency/Central Security Service (NSA/CSS)*, 26 Jan 10

DoDD 5240.01, *DoD Intelligence Activities*, 27 Aug 2007

DoDI O-3115.07, *Signals Intelligence*, 15 Sep 2008

AFDD 2-9, *Intelligence, Surveillance and Reconnaissance Operations*, 17 July 2007

AFMD 15, *Air Force Intelligence, Surveillance and Reconnaissance Agency (AF ISR Agency)*, 27 January 2009

HAFMD 1-33, *Deputy Chief of Staff of the Air Force, Intelligence, Surveillance, and Reconnaissance*, 4 Sep 2009

HQ USAF Program Action Directive (PAD) 07-08 Change 4, 1 Oct 2009

NSA/CSS P 1-3, *NSA/CSS Governance*, 10 Sep 2008

NSA/CSS P 10-1, *Test and Evaluation*, 16 Sep 2004

NSA/CSS P 10-3, *NSA/CSS Enterprise Systems Engineering Process*, 30 Dec 2003

NSA/CSS P 10-4/Manual 10-4, *NSA/CSS Capability Deployment Management Process*, 13 Sep 2006

NSA/CSS P 6-3, *NSA/CSS Operational Information Systems Security Policy*, 8 Aug 2006

NSA/CSS M 130-1, *NSA/CSS Operational Information Systems Security Manual*, 2 Jan 2001

Electronic Security Command/Assistant Chief of Staff for Intelligence (XOI) MOA with NSA/CSS, *MOA Concerning JTAD and JTIDS Program*, Aug 1986

Air Force Intelligence Agency MOU with NSA/CSS National-Tactical Integration Office, *MOU for Joint Interoperability and Engineering organizations*, 10 Feb 2004

NSA/CSS Policy 1-23, *Procedures Governing NSA/CSS Activities That Affect U.S. Persons*, 27 Dec 2007

NSA/CSS SP0002, *The USSID System*, 14 Oct 2008

NSA/CSS SP0018, *Legal Compliance and Minimization Procedures*, 27 Jul 1993

NSA/CSS SIGINT Directorate Directive 406, *Classified*

(Added-AFISRA) USSID CR1501, *Handling of Critical Information (CRITIC)*, 13 August 2009

USSID SP0001, *SIGINT Operating Policy*, 13 June 1994

(Added-AFISRA) *Adopted Forms*

(Added-AFISRA) AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFCO—Air Force Cryptologic Office

AF SCO—Air Force Service Cryptologic Organization

AFDD—Air Force Doctrine Document

AFI—Air Force Instruction

AF ISR Agency—Air Force Intelligence, Surveillance and Reconnaissance Agency

(Added-AFISRA) AFISRA—Air Force Intelligence, Surveillance and Reconnaissance Agency

AFMD—Air Force Mission Directive

AFMAN—Air Force Manual

AFPD—Air Force Policy Document

AFRC—Air Force Reserve Command

AF SCC—Air Force Service Cryptologic Component

(Added-AFISRA) AFRIMS—Air Force Records Management System

AIA—Air Intelligence Agency

(Added-AFISRA) AMOC—Alaskan Mission Operations Center

ANG—Air National Guard

(Added-AFISRA) AOR—Area of Responsibility

(Added-AFISRA) ARC—Air Reserve Component

(Added-AFISRA) C&SRL—Compliance and Standardization Requirements List

CCP—Consolidated Cryptologic Program

CIO—Chief Information Officer

(Added-AFISRA) CML—Crew Manning Letters

(Added-AFISRA) CRITIC—Critical Information

(Added-AFISRA) CTEP—CRITIC Testing and Evaluation Program

DIRNSA/CHCSS—Director, National Security Agency / Chief, Central Security Service

DoD—Department of Defense

DoDI—Department of Defense Instruction

ESC—Electronic Security Command

HHQ—Higher Headquarters

HRMS—Human Resources Management System

IA—Information Assurance

(Added-AFISRA) IAW—In Accordance With

IC—Intelligence Community

ISR—Intelligence, Surveillance and Reconnaissance

(Added-AFISRA) JCS—Joint Chiefs of Staff

JIOC—Joint Information Operation Center

MAJCOM—Major Command

MRA—Mission Resource Authorities

NAF—Numbered Air Force

NCR—National Capitol Region

NSA—National Security Agency

NSA/CSS—National Security Agency/Central Security Service

(Added-AFISRA) OPLAN—: Operational Plan

(Added-AFISRA) OPR—: Office of Primary Responsibility

PA—Privacy Act

(Added-AFISRA) PEC—: Program Element Code

RDS—Air Force Records Disposition Schedule

RDT&E—Research, Development, Test & Evaluation

(Added-AFISRA) SCC—: Service Cryptologic Component

SECDEF—Secretary of Defense

SFA—Senior Functional Authority

SIGINT—Signals Intelligence

(Added-AFISRA) TDY—: Temporary Duty

USAF—United States Air Force

USAFSS—United States Air Force Security Service

USCS—United States Cryptologic System

USSID—United States Signals Intelligence Directive

USSOCOM—United States Special Operations Command

USSS—United States SIGINT System

Terms

Air Force Service Cryptologic Component (AF SCC):—Term used to designate collectively those elements of the USAF that perform cryptologic functions. The term applies to the cryptologic staff of AF ISR Agency, its subordinate elements, and integral cryptologic elements of USAF tactical or combat commands. The AF SCC Commander represents the interests of USAF cryptologic forces to DIRNSA/Chief, Central Security Service (NSA/CSS).

Consolidated Cryptologic Program (CCP): CCP is the portion of the national intelligence program (NIP) managed by the DIRNSA/Chief, CSS. The CCP funds the worldwide **SIGINT operations**—exploitation of foreign communications and non-communications signals to satisfy national-level SIGINT requirements for the U.S. Government--and the national-level operations of the Central Security Service (CSS). Director, National Intelligence (DNI) and the Undersecretary of Defense for Intelligence (USD(I)) provide oversight of the CCP.

Cryptologic:—Activities that include Signals Intelligence and Information Assurance

Intelligence Community (IC):—IC members include the Service Intelligence Organizations (Service Cryptologic Components (SCCs)), NSA, CIA, DIA, NRO, and NGA, as well as Coast Guard Intelligence, Department of Energy, Department of Homeland Security, Department of State, Department of Treasury, and Federal Bureau of Investigation.

Signals Intelligence (SIGINT): A category of intelligence comprising all communications intelligence, electronics intelligence, and foreign instrumentation signal intelligence, however transmitted. (JP 1—02)

United States Signals Intelligence Directive (USSID):—SIGINT policies and procedures for United States Government departments and agencies to follow when appropriately performing SIGINT activities in order for the SIGINT mission of the US to be accomplished in the most efficient and effective manner.

United States SIGINT System (USSS): The unified organization of signals intelligence activities under the direction of DIRNSA/CHCSS. It consists of the NSA/CSS, the

components of the Military Services and the USCG who are authorized to conduct signals intelligence, and such other entities authorized by the Secretary of Defense or DIRNSA/CHCSS to conduct SIGINT activities. (JP 1—02)

Attachment 2—AF ISR Agency Contact Information

CC: afisra.dse@lackland.af.mil, Comm: 210—977-2061, DSN: 969-2061

CV: afisra.dse@lackland.af.mil, Comm: 210—977-2061, DSN: 969-2061

A1: afisra.a1.tm@lackland.af.mil, Comm: 210—977-309/2665, DSN 969-309/2665

A2: afisraa2.taskmanager@lackland.af.mil, Comm: 210—977-6693, DSN: 969-6693

A3: afisra.a3.tm@lackland.af.mil, Comm: 210—977-6751, DSN: 969-6751

A4/7: [afisra.a47—2@lackland.af.mil](mailto:afisra.a47-2@lackland.af.mil), Comm: 210-977-2130, DSN: 969-2130

A5/8: afisra58.workflow@lackland.af.mil, Comm: 210—977-2791, DSN: 969-2791

A6: afisra.a6t@lackland.af.mil, Comm: 210—977-2658, DSN: 969-2658

AFCO Contact Information—Director: afco.exec@nsa.gov, Comm: 301-688-7078, DSN: 644-7078

Deputy Director: afco.exec@nsa.gov, Comm: 301—688-7078, DSN: 644-7078

Director of Staff: afco.exec@nsa.gov, Comm: 301—688-7078, DSN: 644-7078

A1/5/8: afco.a158@nsa.gov, Comm: 301—688-6712/6713, DSN: 644-6712/6713

A3: afco.a3@nsa.gov, Comm: 301—688-5724/5725, DSN: 644-5724/5725

A6: afco.a4@nsa.gov, Comm: 301—688-5441, DSN: 644-5441